IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Cristian Constantinof
Serial No. 10/606,687
Filed: 06/26/2003
For: **EMERGENCY SERVICES FOR PACKET NETWORKS**

Examiner: Nguyen, Quynh H.
Art Unit: 2614

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

DECLARATION UNDER 37 C.F.R. § 1.131 OF BENJAMIN S. WITHROW

1. My name is Benjamin S. Withrow of the law firm of Withrow & Terranova, PLLC, and I am a registered U.S. patent attorney, Registration No. 40,876.

2. Starting in 2000, and continuing until the present time, I have been retained as outside counsel for Nortel Networks Limited (hereinafter "Nortel"), the assignee of the present application.

3. Barring instructions to the contrary, I prepare applications in the order in which they are received from Nortel.

4. On or about February 5, 2003, Nortel requested that I prepare and file the above-referenced application (hereinafter "the present application"). Along with the request to prepare and file the present application, Nortel sent an invention disclosure which described the claimed features of the present application (attached as Appendix A).

5. At the time Nortel requested preparation and filing of the present application, I had a number of other applications (hereinafter "prior applications") on my docket which had to be prepared and filed prior to the preparation and filing of the present application. Accordingly, between about February 5, 2003 and April 7, 2003 I diligently and personally prepared the prior applications in substantially the order in which they were received.

6. On or about April 8, 2003, as evidenced by Appendix B, which is a matrix illustrating various actions taken with respect to the preparation and filing of the present application, which is attached herewith, in the column entitled "Met with inventor," I began preparing the present application. I began the preparation of the present application after I completed the prior applications. I completed a first draft of the application on or about May 19, 2003, which my assistant, Jennifer Alkove, subsequently sent to Cristian Constantinof on May 19, 2003, as evidenced by Appendix B, in the column entitled "First draft sent."

7. On or about June 9, 2003, I received comments from Cristian Constantinof, as evidenced by Appendix B, in the column entitled "First draft received back." I incorporated these comments into a second draft of the present application and sent the second draft of the present application to in-house counsel at Nortel on June 11, 2003, as evidenced by Appendix B, in the column entitled "Final draft sent."

8. On June 25, 2003, I received Final draft comments back and on June 26, 2003, I filed the present application with the U.S. Patent and Trademark Office.

9. I hereby declare that all declarations made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Benjamin S. Withrow

December 19, 2007
Date

Appendix A

Nortel Networks Confidential & Privileged In formation

Invention Disclosure Submission Reply

Disc No:	15780RO	Received Date:	13 dec 2002
Disclosure Title:	Method and Apparatus for Session Control and Emergency Services in SIP Networks		

---=== Inventors ===---

Global Id	Name	Work Info	Home Info
1666839	**HR Name:** CONSTANTINOF, CRISTIAN **Known As:** CRISTIAN **Email:** chrisc@nortelnetworks.com **Mgr First Name:** JOHN **Mgr Last Name:** MARLOW **Mgr Global ID:** 0228694	**Location:** 3500 CARLING AVENUE NEPEAN ONTARIO K2H 8E9 CANADA **Location Code:** CAR **Dept:** W628 **Phone:** 3933654 **Ext Phone:** 763-3654 **Fax:** **Ext Fax:** **MailStop:** 04352F10 **Citizenship:** CANADA	**Address:** 13 FOXLEIGH KANATA, ON CANADA K2M 1B4 **Phone:** 06135927246

---=== Attachments ===---

File Name	File Type	File Comments
Overload_Prelim_V03.doc	Microsoft Word (*.doc)	

<End of Attachments>

Were there additional inventors involved:	no	Was there contractor involvement:	no
Name of Supervisor or Divisional Head:		Name of VP:	
MARLOW JOHN		DODD RANDY	
LOB:	WIRELINE NETWORKS	Business Unit:	Application Service Providers
Conception Date:			
Has this invention been discussed with others? If so, please complete:			
Inside Nortel - Whom?	DANY SYLVAIN, MATT VELLA, PAUL WILSON, ROBERT PUGH	Outside Nortel - Whom?	
Inside Nortel - When?	02 dec 2002	Outside Nortel - When?	
NDA?	no		

Are you aware of any imminent future disclosures? Please provide dates and details:	
Keywords for Searching:	**Products that will use this invention:**
Session Control, SIP, Overload, denial of service, Emergency Service, SIP event notification, SIP session filter	Succession and IMS products: CS2000, CS2000c, IMS, USP
Does this invention arise from any arrangement involving an external organization?	no
Is this invention relevant to a Standards Activity?	**Internal Funding Project #'s:**
yes	

Technical Information

Brief Description of the Invention:

Session Control

The proposed solution defines a SIP-based mechanism that enables SIP Proxy Servers and User Agents, or network administrators, to inform other SIP network elements about special node conditions (overload, malicious calls, etc.) and to request corrective actions. The solution also defines a new SIP network element, the SIP Session Filter (SSF), which performs SIP screening function based on special condition information received from Proxy Servers and User Agents, or from network administrators.

Emergency Services

The proposed solution defines a SIP-based method that enables service providers operating SIP networks to identify and tag INVITE messages requesting the establishment of emergency services sessions. The solution also defines a new SIP functional element, the SIP Emergency Proxy (SEP), responsible for identifying and tagging emergency session requests in a secure way that prevents abusive or malicious use of emergency services.

Problem Solved by the Invention:

Session Control

The volume of calls in a telephony network varies widely in time and, traditionally, networks have been engineered to support peak traffic levels associated with social or business calling patterns. There are, however, certain events that will generate traffic patterns that exceed the supported peak levels, such as, for example: mass calling events triggered by a promotional/advertising campaigns, catastrophic events (earthquakes, acts of war, etc.), switch malfunctioning, and denial of service attacks. Left unchecked, such events may disable individual switches and significantly impact the throughput of the entire network. Furthermore, malicious service requests may attempt to disrupt normal service by disabling proxy servers or end user agents in the network.

The role of network session controls is to localize the effect of unexpectedly high traffic levels or malicious session requests and to maintain the agreed service levels for customers. While individual switches may implement nodal session control mechanisms, the network session controls help to isolate the source of undesired session requests and to minimize the impact on other calls.

Traditionally network call / session controls for overload situations have been addressed in TDM telephony networks by two mechanisms intended to throttle the call volume arriving to a given switch:

? Trunk group management ? dynamically reducing the number of trunks available between switches

? ISUP signaling screening in STPs ? filtering call setup requests based on point codes, calling or called number, etc.

In SIP networks neither mechanism is applicable since SIP softswitches do not have the concept of trunk groups and there are no STPs.

Due to their open nature, SIP networks may also vulnerable to malicious attacks executed under the guise of session establishments. It is, therefore, important to develop a protection mechanism that allows service providers to limit or prevent certain service requests from being propagated through the network.

Emergency Services

Providing emergency services in overload conditions is especially challenging since service providers have to ensure that emergency calls are established regardless which other calls are filtered out. In the present telephony network there are mechanisms to identify calls made from/to special locations involved in providing emergency services (911, police, hospitals, fire stations, government agencies, etc.). Network resources (trunks) are reserved to ensure completion of these calls and the call set-up requests are given processing priority within se switching nodes.

As SIP technology is increasingly deployed to establish communication sessions, a method for addressing emergency services requirements has to be made available for SIP networks. The solution for emergency services has to ensure that emergency SIP sessions are established with the highest priority, regardless of network overload conditions, and that the system is not open to abuse from malicious users.

Solutions that have been tried and why they didn't work:

Session Control

The only SIP session / overload control solutions considered today are:

? Discarding incoming SIP messages ? Affects not only new session establishment attempts but also sessions in the process of being established

? Responding with ?Service Unavailable? to incoming INVITE messages ?Requires additional processing effort from the element in overload situation and doesn?t propose any remedial actions to other nodes in the network.

The ISUP based network overload mechanisms relies on the reduction in the number of available circuits terminating on the protected element. This solution is not applicable in the SIP network since there are no circuits in this network

Emergency Services

The SIP protocol supports a ?Priority? header field which may be given the value ?emergency?, but this header field indicates the urgency of the request as perceived by the client. There is no control on who sets the value of the Priority field (opening the potential for abuse), and there is no mandatory action on behalf of the SIP network elements when processing a message with this field set to ?emergency?.

Specific elements or steps that solved the problem and how they do it:

Session Control

The proposed network session control solution consists of one or several SIP Proxy servers or User Agents that have to be protected from overload or other undesired session requests, and a SIP Session Filter (SSF), that can be implemented either on a dedicated network element or on a pre-existing server including, potentially, even on the elements to be protected.

? The Protected Element, or a network administrator, informs the SSF when an overload / undesired session condition occurs.

? Upon receiving an event information, the SSF applies back pressure to incoming INVITE messages meeting the event criteria by responding with ?System Protection? responses to, or by ignoring, some or all of those INVITE messages.

? The SSF may forward the event information referencing a protected element to the SIP network elements that send INVITE requests addressed to the protected element. The information may be transmitted via provisional or final responses to INVITE messages, INFO messages, new ?System Protection? response, BYE message, etc.

? Upon recognizing the termination of an offending condition, the SSF ceases to apply back pressure on INVITE messages meeting the event criteria.

Emergency Services

The proposed Emergency services solution is based on the deployment of a SIP Emergency Proxy (SEP) that can be implemented either on a dedicated network element or on a pre-existing server.

Upon receiving an INVITE request, the SEP verifies if the request meets the criteria of an emergency service request. If the criteria are met, the SEP adds to the INVITE message an Emergency header field having as value the level of emergency as well as additional information that uniquely identifies the call, such as Call ID, To and From value, etc. The call-identifying information is the same for all SEPs in a given service provider network.

For security reasons, to avoid malicious / unauthorized use of Emergency services, the SEP value of the Emergency header may be encrypted. A service provider may use a Private Key encryption mechanism and distribute the encryption key to other SIP elements in the network, or they may use a Public Key encryption mechanism, to minimize the potential for security breach. With the Public Key security mechanism, the SEP encrypts the field value with its private key, but other SIP elements may decrypt the value using a known public key.

Commercial value of the invention to Nortel and Nortel's major competitors:

The proposed solutions

? Accelerate industry acceptance of VoIP technology and creates market demand for Succession products

? Leverage overload protection mechanisms implemented in CS2000 servers providing a competitive advantage for the Succession solution

? Create demand for a SIP Session Filter and SIP Emergency Proxy elements that can be successfully implemented on the CS2K, IMS and USP platform

Method and Apparatus for Session Control and Emergency Services in SIP Networks

Author: Cristian Constantinof

Problem Statement

Session Control

The volume of calls in a telephony network varies widely in time and, traditionally, networks have been engineered to support peak traffic levels associated with social or business calling patterns. There are, however, certain events that will generate traffic patterns that exceed the supported peak levels, such as, for example: mass calling events triggered by a promotional/advertising campaigns, catastrophic events (earthquakes, acts of war, etc.), switch malfunctioning, and denial of service attacks. Left unchecked, such events may disable individual switches and significantly impact the throughput of the entire network. Furthermore, malicious service requests may attempt to disrupt normal service by disabling proxy servers or end user agents in the network.

The role of network session controls is to localize the effect of unexpectedly high traffic levels or malicious session requests and to maintain the agreed service levels for customers. While individual switches may implement nodal session control mechanisms, the network session controls help to isolate the source of undesired session requests and to minimize the impact on other calls.

Traditionally network call / session controls for overload situations have been addressed in TDM telephony networks by two mechanisms intended to throttle the call volume arriving to a given switch:

- Trunk group management – dynamically reducing the number of trunks available between switches
- ISUP signaling screening in STPs – filtering call setup requests based on point codes, calling or called number, etc.

In SIP networks neither mechanism is applicable since SIP softswitches do not have the concept of trunk groups and there are no STPs.

Due to their open nature, SIP networks may also vulnerable to malicious attacks executed under the guise of session establishments. It is, therefore, important to develop a protection mechanism that allows service providers to limit or prevent certain service requests from being propagated through the network.

Emergency Services

Providing emergency services in overload conditions is especially challenging since service providers have to ensure that emergency calls are established regardless which other calls are filtered out. In the present telephony network there are mechanisms to identify calls made from/to special locations involved in providing emergency services (911, police, hospitals, fire stations, government agencies, etc.). Network resources (trunks) are reserved to ensure completion of these calls and the call set-up requests are given processing priority within se switching nodes.

As SIP technology is increasingly deployed to establish communication sessions, a method for addressing emergency services requirements has to be made available for SIP networks. The solution for emergency services has to ensure that emergency SIP sessions are established with the highest priority, regardless of network overload conditions, and that the system is not open to abuse from malicious users.

Solutions State of the Art

Session Control

The only SIP session / overload control solutions considered today are:

- Discarding incoming SIP messages – Affects not only new session establishment attempts but also sessions in the process of being established
- Responding with "Service Unavailable" to incoming INVITE messages –Requires additional processing effort from the element in overload situation and doesn't propose any remedial actions to other nodes in the network.

The ISUP based network overload mechanisms relies on the reduction in the number of available circuits terminating on the protected element. This solution is not applicable in the SIP network since there are no circuits in this network

Emergency Services

The SIP protocol supports a "Priority" header field which may be given the value "emergency", but this header field indicates the urgency of the request as perceived by the client. There is no control on who sets the value of the Priority field (opening the potential for abuse), and there is no mandatory action on behalf of the SIP network elements when processing a message with this field set to "emergency".

Proposed Solution

Session Control

The proposed solution defines a SIP-based mechanism that enables SIP Proxy Servers and User Agents, or network administrators, to inform other SIP network elements about special node conditions (overload, malicious calls, etc.) and to request corrective actions. The solution also defines a new SIP network element, the SIP Session Filter (SSF), which performs SIP screening function based on special condition information received from Proxy Servers and User Agents, or from network administrators.

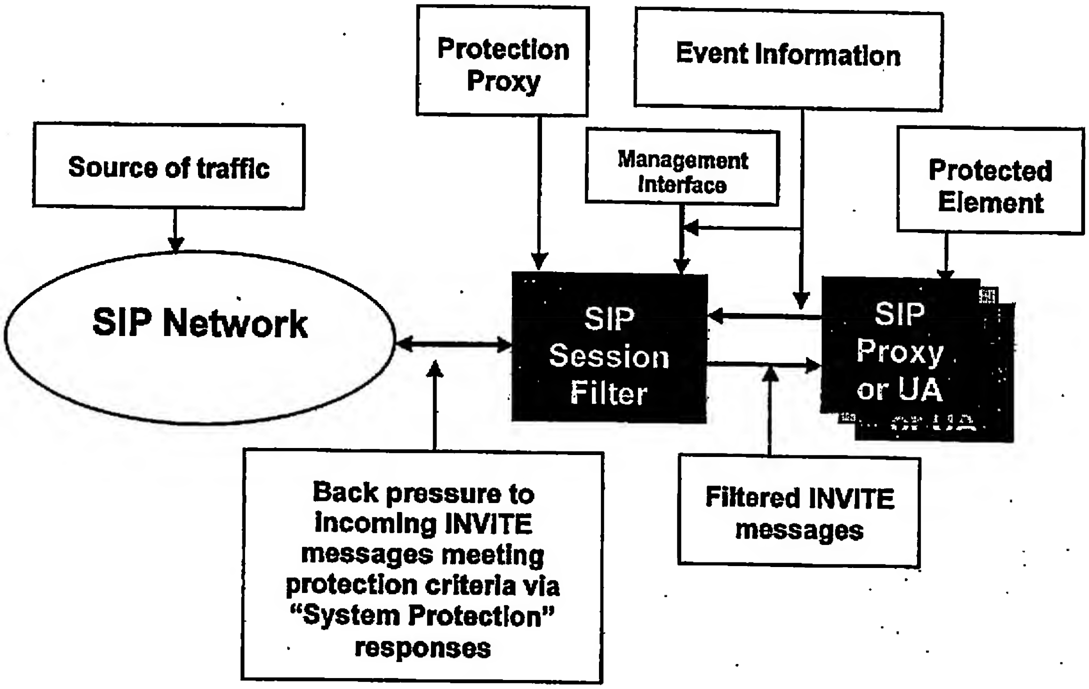
Emergency Services

The proposed solution defines a SIP-based method that enables service providers operating SIP networks to identify and tag INVITE messages requesting the establishment of emergency services sessions. The solution also defines a new SIP functional element, the SIP Emergency Proxy (SEP), responsible for identifying and tagging emergency session requests in a secure way that prevents abusive or malicious use of emergency services.

Solution Description

Session Control

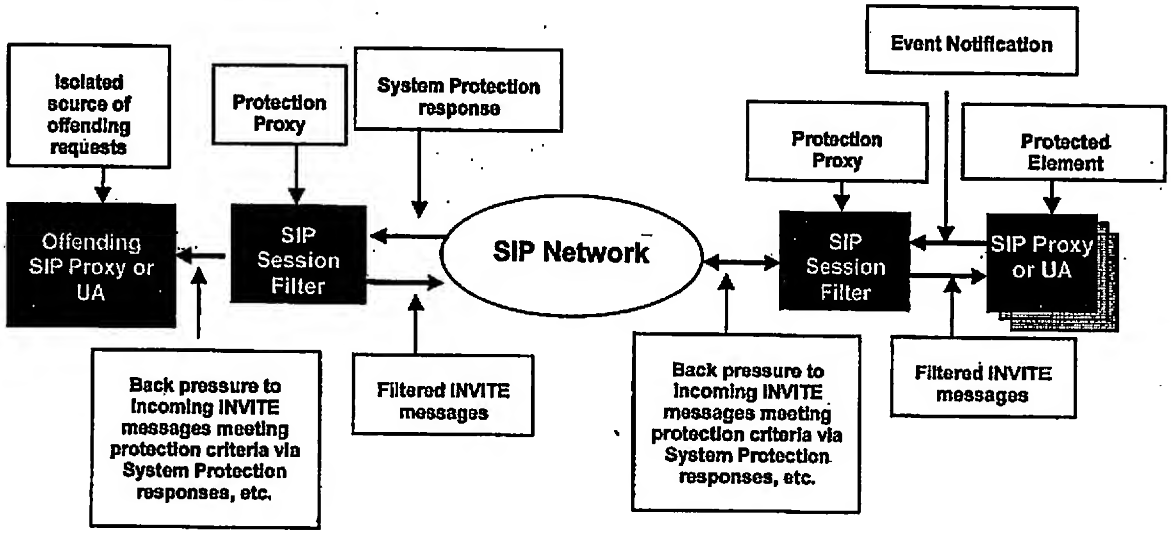
The proposed network session control solution consists of one or several SIP Proxy servers or User Agents that have to be protected from overload or other undesired session requests, and a SIP Session Filter (SSF), that can be implemented either on a dedicated network element or on a pre-existing server including, potentially, even on the elements to be protected. In the latter case, the event notification mechanism between the protected element and the co-resident SSF is an internal, implementation-dependent interface.



- The SIP Session Filter (SSF) acts as a proxy server for all call legs established with the Protected Element.
- The Protected Element may be informed of the existence of the SSF (through provisioning, or dynamically by the SSF using the Subscribe/Notify protocol)
- The Protected Element informs the SSF when an overload / undesired session condition occurs. The event information may be sent using the Notify method of the Subscribe / Notify protocol, or via another appropriate SIP message (e.g. in the provisional or final responses to INVITE messages, INFO messages, new "System Protection" final response, BYE message, etc.). The event information may apply to all incoming session requests or may identify a specific subset of offending requests based on criteria such as the source or destination URI of the offending request, subject, etc. The event information may specify explicitly or

implicitly the reduction level expected for the flow of incoming INVITE messages meeting the offending session criteria. For the use of the Subscribe / Notify mechanism, an event package defining the offending condition has to be defined to specify the offending condition, filtering criteria for INVITE messages, and required actions and reduction criteria. For the use of SIP messages, a Session_Control header may be defined to include several parameters describing the offending condition, filtering criteria for INVITE messages, and required actions and reduction criteria.

- The reduction criteria may be expressed in various ways, including:
  - a reduction "level", where the measurement associated with the level is established by the SSF
  - a reduction percentage, identifying the INVITE messages to be filtered out within a given timeframe
  - a maximum allowed number of simultaneous sessions
- Alternatively, event information may be delivered to the SSF via commands issued by an operator through a management user interface
- Upon receiving an event information, the SSF applies back pressure to incoming INVITE messages meeting the event criteria by responding with "System Protection" responses to, or by ignoring, some or all of those INVITE messages.
- The SSF may forward the event information referencing a protected element to the SIP network elements that send INVITE requests addressed to the protected element. The information may be transmitted via provisional or final responses to INVITE messages, INFO messages, new "System Protection" response, BYE message, etc. The capability of a SSF to forward event information to other SIP network elements enables service providers to limit the propagation of abnormal or malicious session requests through the network. This can be done by deploying SSFs close to points in the network that may generate the undesired traffic.


Isolated source of offending requests
Protection Proxy
System Protection response
Event Notification
Protection Proxy
Protected Element
Offending SIP Proxy or UA
SIP Session Filter
SIP Network
SIP Session Filter
SIP Proxy or UA
Back pressure to incoming INVITE messages meeting protection criteria via System Protection responses, etc.
Filtered INVITE messages
Back pressure to incoming INVITE messages meeting protection criteria via System Protection responses, etc.
Filtered INVITE messages

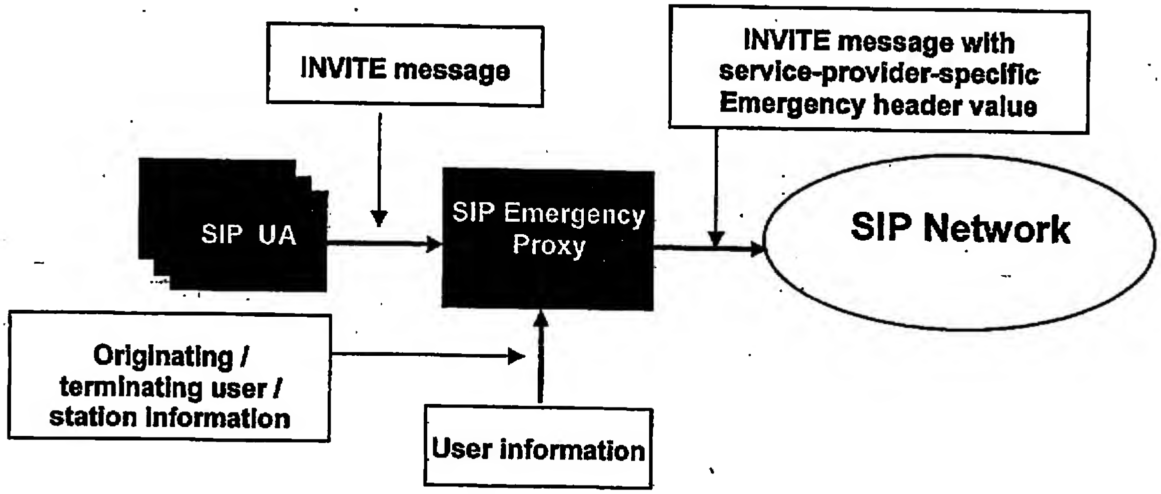
-

- The SSF may receive subsequent event notifications from (or with reference to) the protected element. A notification for a previously flagged condition may request a higher filtering level/percentage or a reduced number of allowable simultaneous sessions.
- The Protected Element informs the SSF when the offending condition ends. The information may be sent using the Notify method of the Subscribe/Notify protocol or via other SIP messages (e.g. provisional or final responses to INVITE messages, INFO messages, BYE message, etc.)
- Alternatively the SSF may consider the termination of the offending condition at the expiration of a timer set upon receiving the event notification. The duration of the timer may be predetermined or may be specified as part of the event notification.
- The SSF may also be informed of the termination of an offending condition via commands issued by an operator through a management user interface.
- Upon recognizing the termination of an offending condition, the SSF ceases to apply back pressure on INVITE messages meeting the event criteria.

Two types of "hybrid" SSF can be implemented on SIP network elements that provide an interface to the PSTN.

- **ISUP throttling hybrid SSF** - Such an implementation receives the event notification from the protected SIP network element and sends ISUP Overload messages (OLM) in response to incoming IAM messages.
- **SIP throttling hybrid SSF** - Such an implementation receives overload notification from a protected ISUP network element, filters incoming SIP INVITE messages and sends System Protection SIP responses.

Emergency Services


INVITE message
INVITE message with service-provider-specific Emergency header value
SIP UA
SIP Emergency Proxy
SIP Network
Originating / terminating user / station information
User information

The proposed Emergency services solution is based on the deployment of a SIP Emergency Proxy (SEP) that can be implemented either on a dedicated network element or on a pre-existing server.

Upon receiving an INVITE request, the SEP verifies if the request meets the criteria of an emergency service request. If the criteria are met, the SEP adds to the INVITE message an Emergency header field having as value the level of emergency as well as additional information that uniquely identifies the call, such as Call ID, To and From value, etc. The call-identifying information is the same for all SEPs in a given service provider network.

For security reasons, to avoid malicious / unauthorized use of Emergency services, the SEP value of the Emergency header may be encrypted. A service provider may use a Private Key encryption mechanism and distribute the encryption key to other SIP elements in the network, or they may use a Public Key encryption mechanism, to minimize the potential for security breach. With the Public Key security mechanism, the SEP encrypts the field value with its private key, but other SIP elements may decrypt the value using a known public key.

Two types of "hybrid" SEP can be implemented on SIP network elements that provide an interface to the PSTN.

- **ISUP detecting SEP** - Such an implementation detects Emergency services requests arriving from the PSTN via ISUP requests and maps them to SIP INVITE requests by using the Emergency header
- **ISUP mapping SEP** - Such an implementation detects Emergency services requests arriving via SIP INVITE requests and maps them to corresponding emergency ISUP requests

When a SIP network element receives an INVITE with an Emergency header, it may decide to process the Emergency information. After decrypting the Emergency header value, the network element may take specific routing or presentation actions depending on the emergency value.

INVITE messages with a valid Emergency header shall not be discarded by SSFs, even if they meet the discard criteria.

Claims

Session Control

- A Method and apparatus for Session Control in SIP networks
- A method for notifying detection of offending conditions
  - o Non-call-related
    - ▪ Subscribe / Notify
    - ▪ Management user interface
  - o Call related
    - ▪ Response messages to INVITE requests
    - ▪ Other messages (INFO, etc.)
- A method for specifying identification criteria of offending session requests

- A method for notifying termination of offending condition
    - Non-call related
        - Subscribe / Notify
        - Management user interface
    - Call related
        - Response messages to INVITE requests
        - Other messages (INFO, etc.)
- A selective SIP throttling device and procedure for new incoming session requests that doesn't affect established sessions or the processing capabilities of the protected element
- A selective hybrid SIP-ISUP throttling device and procedure for new incoming ISUP IAM requests that responds to offending conditions in the SIP network but doesn't affect established sessions or the processing capabilities of the protected element
- A selective hybrid SIP-ISUP throttling device and procedure for new incoming INVITE requests that responds to overload conditions in the PSTN network but doesn't affect established sessions or the processing capabilities of the element in overload conditions

Emergency Services

- A method and apparatus for providing emergency services in SIP networks
- A mechanism to ensure service provider control over emergency services requests.
- An authentication mechanism that prevents fraudulent use of emergency services
- A mechanism that ensures emergency services requests are forwarded even when SIP elements are in overload conditions.
- A hybrid ISUP-SIP device that detects Emergency services requests arriving from the PSTN via ISUP requests and maps them to SIP INVITE requests by using the Emergency header
- A hybrid ISUP-SIP device that detects Emergency services requests arriving via SIP INVITE requests and maps them to corresponding emergency ISUP requests.

Value Proposition to Service Providers

Session Control

The proposed solution increases the resilience of SIP networks and reduces their vulnerability accidental or malicious events. By deploying the proposed solution service providers may increase the resilience of SIP networks to the same level as their PSTN network and provide an equivalent level of service. This capability will accelerate the migration of voice traffic from circuit to packet networks.

Emergency Services

The proposed solution enables service providers to offer emergency services on a SIP network at the same level that is currently available in the PSTN. This capability will accelerate the migration of voice traffic from circuit to packet networks.

Value Proposition to Nortel Networks

The proposed solutions

- Accelerate industry acceptance of VoIP technology and creates market demand for Succession products
- Leverage overload protection mechanisms implemented in CS2000 servers providing a competitive advantage for the Succession solution
- Create demand for a SIP Session Filter and SIP Emergency Proxy elements that can be successfully implemented on the CS2K, IMS and USP platform

Appendix B

Nortel Case Status

Matter ID	Date of Letter & Fax Confirm	Met with Inventor	First draft sent	First draft received back	Final draft sent (IP Law)	Final draft comments received back (IP Law)	Formal paperwork sent	Formal paperwork received back	Actual filing date (Prov.)
7000-237A	2/5/2003	4/8/2003	5/19/2003	6/9/2003	6/11/2003	6/25/2003	6/11/2003	6/16/2003	6/26/2003